

# ALLEGATO 1. ASL GALLURA CYBERSECURITY GOVERNANCE

**Azienda Socio-Sanitaria Locale n.2 della Gallura**

Sede Legale: via Bazzoni-Sircana, 2/2A – 07026 Olbia (SS)

Tel. 0789/552305 - [www.aslgallura.it](http://www.aslgallura.it)

Posta certificata: [protocollo@pec.aslgallura.it](mailto:protocollo@pec.aslgallura.it)

Codice Fiscale e Partita IVA: 02891650901

**Revisione 00**

## Sommario

|   |                                           |   |
|---|-------------------------------------------|---|
| 1 | Descrizione e Oggetto dell'Allegato ..... | 3 |
|---|-------------------------------------------|---|

## 1 DESCRIZIONE E OGGETTO DELL'ALLEGATO

Il presente allegato descrive la **Linea Guida Operativa per le Politiche di Sicurezza (GV.PO-01)** dell'**ASL Gallura**, definendo il **Modello di Governance**, i **Requisiti Minimi** e le **Procedure di Notifica** necessari per l'adeguamento ai quadri normativi sulla cybersecurity.

Nello specifico, il documento illustra:

- **Inquadramento Normativo e Strategico:** L'allineamento al Framework Nazionale di Sicurezza (NFSC), in conformità con la Direttiva NIS2 (D.Lgs. 138/2024), la Legge 90/2024 e le specifiche dell'Agenzia per la Cybersicurezza Nazionale (ACN).
- **Architettura e Governance Regionale:** Il riparto delle responsabilità tra l'**ASL Gallura** (titolare dei dati, della governance strategica, della compliance e dell'interfaccia con ACN) e **ARES Sardegna** (responsabile della gestione esclusiva dell'infrastruttura ICT, delle reti, dei datacenter, dei servizi SOC/NOC e delle operazioni CSIRT).
- **Organigramma di Governance Locale (ASL Gallura):** L'individuazione formale dei ruoli chiave nominati per la gestione del portale e delle procedure ACN:
  - **Punto di Contatto (PdC):** Ing. Martino Ruiu
  - **Sostituto Punto di Contatto (SPdC):** Ing. Francesca Mura
  - **Segreteria (SG):** Dott. Ciro Soro
  - **Taskforce Tecnica / Referenti CSIRT (ARES Sardegna):** Ing. Mauro Gaviano, Ing. Gianluigi Frau e Sig. Marco Fenudi.
- **Requisiti Minimi e Misure di Protezione:** Le misure di sicurezza previste dal framework ACN (tra cui autenticazione multifattore MFA, protezione endpoint EDR, gestione dei backup offline e controllo della catena di fornitura).
- **Procedure e Flussi di Gestione degli Incidenti:** I tempi tassativi di notifica (segnalazione entro le 24 ore e report completo entro le 72 ore al CSIRT Italia) e il flusso operativo congiunto tra il triage tecnico di ARES e la validazione/notifica dell'ASL.
- **Attuazione e Prossimi Passi:** L'istituzione di un **Tavolo Tecnico Congiunto** ASL-ARES, l'avvio della registrazione sulla piattaforma ACN e l'istituzione formale dell'Ufficio Cyber Sicurezza dell'ASL Gallura.

# LINEA GUIDA OPERATIVA PER LE POLITICHE DI SICUREZZA (GV.PO-01)

---

Modello di Governance, Requisiti Minimi e  
Procedure di Notifica per la Cybersicurezza



# FRAMEWORK NAZIONALE (NFSC)



## **DIRETTIVA NIS2 (D.Lgs. 138/2024)**

Elevazione dei livelli di sicurezza per i soggetti essenziali e importanti. Obbligo di registrazione e anagrafica.



## **LEGGE 90/2024 (28 giugno 2024)**

Disposizioni per il rafforzamento della cybersicurezza nazionale, resilienza delle PA e contrasto ai reati informatici.



## **SPECIFICHE ACN (Settembre 2025)**

Adozione di 11 documenti organizzati, tra cui le Politiche di Sicurezza (GV.PO-01) e l'Organizzazione per la cybersicurezza (GV.RR-02).

# Architettura della Sicurezza Regionale



# Modello di Governance Locale: ASL Gallura



**Punto di Contatto (PdC)**

**Ing. Martino Ruiu**

Direttore SC Tecnologia e Transizione Digitale / RTD. Referente primario ACN. Gestione piattaforma NIS, validazione e invio formale dichiarazioni, attivazione segnalazioni incidenti.



**Sostituto (SPdC)**

**Ing. Francesca Mura**

IFP Telemedicina. Supporto al PdC e subentro in caso di assenza assenza per l'accesso operativo al Portale ACN.



**Segreteria (SG)**

**Dott. Ciro Soro**

Collaboratore Professionale Analista. Gestione operativa, supporto amministrativo e aggiornamento anagrafico.

# Taskforce Tecnica Centralizzata: ARES Sardegna

In base alla **L.R. 24/2020**, l'ICT è attribuito in via esclusiva ad **ARES**.

Il presidio tecnico di raccordo con CSIRT Italia opera tramite il **Dipartimento di Sanità Digitale e Innovazione Tecnologica** (SSD Sicurezza ICT).

## Referenti CSIRT ARES

**Ing. Mauro Gaviano**

**Ing. Gianluigi Frau**

**Sig. Marco Fenudi**

*ARES garantisce l'esecuzione del modello regionale di gestione centralizzata dei servizi di cybersicurezza.*

# Riparto delle Competenze e Responsabilità

| Funzione Strategica/Operativa                      | ASL Gallura | ARES Sardegna          |
|----------------------------------------------------|-------------|------------------------|
| Titolarità delle Politiche di Sicurezza (GV.PO-01) | ✓           | Supporto               |
| Gestione Operativa Reti e Datacenter               | -           | ✓                      |
| Aggiornamento Piattaforma ACN/NIS                  | ✓ (via PdC) | -                      |
| Rilevamento tecnico degli incidenti (SOC)          | -           | ✓                      |
| Notifica formale incidenti a CSIRT Italia          | ✓           | Fornitura Dati Tecnici |

**Takeaway:** La conformità normativa richiede un'azione simbiotica:  
ARES implementa le misure tecniche, ASL governa e certifica la compliance.

# Requisiti Minimi di Sicurezza (Framework ACN)

**ID.RA-05**



## Rischio

Analisi periodica dei rischi per i sistemi informativi e di rete rilevanti, inclusa la catena di fornitura.

**PR.AA-03**



## Accessi

Implementazione di Multi-Factor Authentication (MFA) o autenticazione continua per l'accesso ai sistemi.

**PR.DS-11**



## Continuità

Gestione strutturata dei backup, con isolamento offline e test ciclici di ripristino.

**DE.CM-09**



## Endpoint

Sistemi attivi per il rilevamento e blocco di codice malevolo sui punti terminali.

**GV.SC-01**



## Fornitori

Valutazione e monitoraggio della sicurezza nei contratti di acquisizione di beni e servizi ICT.

# Focus Tecnico: Protezione e Resilienza Infrastrutturale



## Layer 1: Autenticazione (PR.AA-03)

MFA obbligatoria. Fatte salve motivate ragioni tecniche, l'accesso richiede fattori multipli.

## Layer 2: Protezione Attiva (DE.CM-09)

EDR/Antivirus avanzato su tutti i dispositivi. Rilevamento continuo delle anomalie.

## Layer 3: Backup Offline (PR.DS-11)

Copie di sicurezza isolate dalla rete principale. Fondamentale contro ransomware, con test di ripristino.

# La Gestione degli Incidenti: Il Fattore Tempo

TLP: CLEAR



**T=0: Rilevamento**  
Evidenza dell'incidente  
tramite monitoraggio ARES  
o segnalazione ASL.

1

2

**T+1h / T+6h: Incidenti  
Critici (ICP-A/B)**

Segnalazione immediata per  
incidenti ad alto impatto  
(DPCM 81/2021).

1

**T=0: Rilevamento**  
Evidenza dell'incidente  
tramite monitoraggio ARES  
o segnalazione ASL.

3

**T+24h: Notifica Iniziale  
Obbligatoria**

Compilazione del modulo  
CSIRT Italia. Finestra critica  
per compliance PSNC.

4

**T+72h: Notifica Completa**

Invio report dettagliato su  
indicatori di compromissione  
e impatto sul business.

**Curva di Attivazione**

# Flusso Operativo di Segnalazione (Entro le 24 Ore)

## 1. Rilevamento & Triage (ARES / SOC)

Analisi dell'impatto sui beni ICT o sistemi contigui. Classificazione dell'incidente.

## 2. Attivazione Governance (ASL)

Comunicazione immediata all'Ing. Martino Ruiu (PdC) e alla Segreteria.

## 3. Raccolta Dati (Congiunta)

Definizione di: Data/ora, Asset impattati, Vettori d'attacco, Indicatori di Compromissione (IOC), e isolamento delle evidenze.

## 4. Compilazione CSIRT (ASL)

Inserimento dati nel modulo portale ACN/CSIRT da parte del Punto di Contatto.

# L'Ecosistema di Sostegno: ARES Sardegna ha aderito agli Accordi quadro Consip ID 2296

## **Lotto 1** **(Sicurezza da Remoto)**

Copertura delle misure operative continuative. Attivazione dei servizi di Security Operation Center (SOC) e Next Generation NOC gestiti in capo ad ARES.

## **Lotto 2** **(Compliance e Controllo)**

Supporto strategico per ARES e le 8 ASL regionali. Include l'analisi dello status quo, ridisegno della Security Strategy, e gestione della compliance normativa (GDPR, NIS2, Legge 90/2024).

# Il Motore della Compliance: Il Tavolo Tecnico Congiunto



**MANDATO:** Urgente istituzione di un tavolo tecnico congiunto tra i referenti ASL e i referenti CSIRT di ARES.

**Obiettivo:** Garantire efficacia, tempestività, allineamento operativo e il rispetto delle scadenze improrogabili definite dall'ACN.

# Chiusura e Prossimi Passi Operativi

1

## Registrazione ACN

Completamento degli adempimenti sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale a cura del PdC (Ing. Ruiu).

2

## Costituzione Ufficio

Istruzione dell'atto formale per la costituzione dell'Ufficio della Cyber Sicurezza della ASL Gallura, da definire in stretta intesa con ARES Sardegna.

3

## Procedure di Resilienza

Dettaglio finale dei compiti assegnati e delle procedure di continuità (ID.IM-04) in caso di attacco, supportati dal framework Consip.